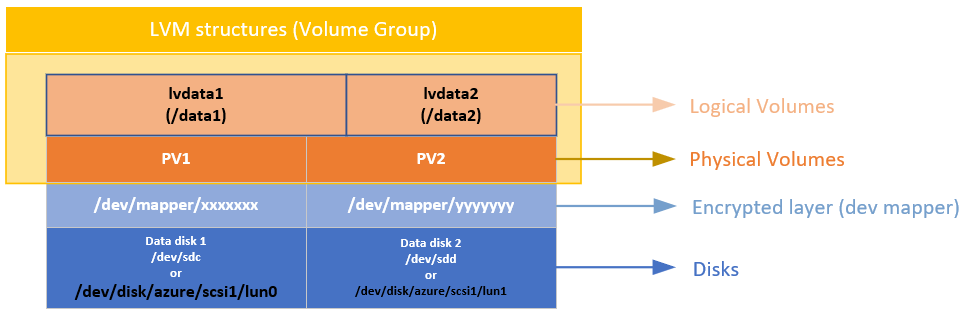
**Scenario**

**This scenario is applicable to ADE dual-pass and single-pass extensions, however, keep under consideration that ADE dual pass should no longer be used on new ADE encryptions since it is on deprecation path**

This document is a step by step process about how to perform LVM on crypt configurations.

When using LVM on crypt you will be following the process outlined below:

1. The corresponding data disks are attached to the corresponding VM
2. The corresponding LUNs/Disks are configured (a file system is created on top of each LUN), temporary mount points are created, they are added to /etc/fstab and they are mounted
3. Those disk(s) or underlying device(s) are encrypted using volume\_type=Data (where only data file systems are going to be encrypted) or volume\_type=ALL (where both OS and Data disks are encrypted).
   1. [EncryptFormatAll](https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-linux#-use-encryptformatall-feature-for-data-disks-on-linux-iaas-vms) option will be used.
4. Once the underlying device(s) are encrypted then the LVM structures are created on top of that encrypted layer
   1. The Physical Volumes (PV) are created on top and those are used to create the corresponding volume group
   2. The volumes are created and added to /etc/fstab as any other normal LVM file system



**Environment**

* Linux distributions

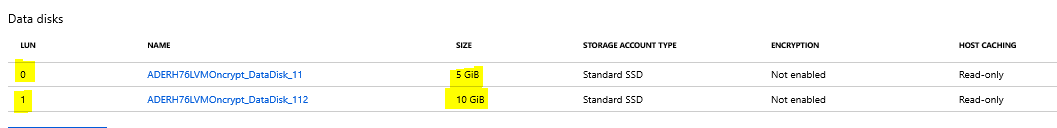
**Procedure**

**Pre-requisites for data disk setup**

1. First, prior to enabling encryption, the data disks to be encrypted need to be properly listed in /etc/fstab and must be mounted
2. Next, ensure that the /etc/fstab settings are configured properly for mounting, use UUIDs instead of device names given device names are not persistent.
3. EncryptFormatAll is mandatory to be used to encrypt the devices.
4. Check the output of the *lsblk* and *df -h* commands to verify that the desired disk is already mounted.
5. Once the data disk is ready, you can choose to either encrypt the existing data block-by-block using EnableEncryption using EncryptFormatAll.

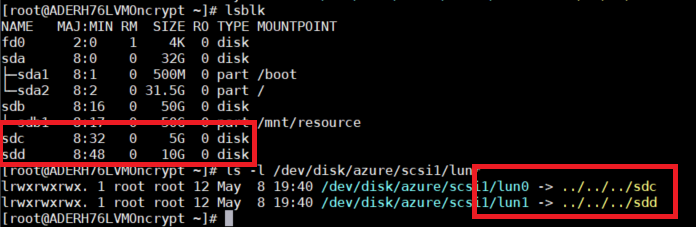
**Preparing the virtual machine**

1. For this test, we created a VM Standard D2s v3 (2 vcpus, 8 GB memory) with 2 data drives (with 5GB and 10GB respectively)
2. Identify the disks you allocated to the virtual machine using the following commands
   1. You can see they are related to the LUN ID shown in the portal disks blade:



# lsblk

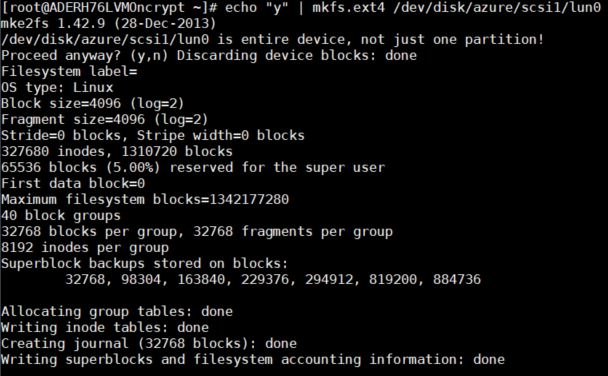
# ls -l /dev/disk/azure/scsi1/lun\*

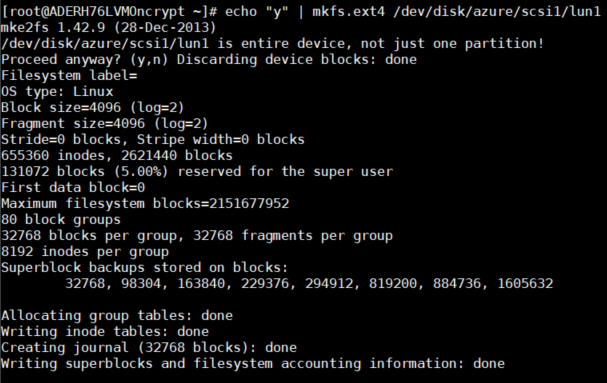


1. Format and mount each azure LUN that will be used by LVM data VGs and add them to /etc/fstab
   1. Format each of the LUNs that will be used by LVM after the encryption, make sure you use the azure paths in the form /dev/disk/azure/scsi1/lun# as shown below.

# echo "y" | mkfs.ext4 /dev/disk/azure/scsi1/lun0

# echo "y" | mkfs.ext4 /dev/disk/azure/scsi1/lun1





* 1. Add them to /etc/fstab using the following commands:

# UUID0="$(blkid -s UUID -o value /dev/disk/azure/scsi1/lun0)"

# UUID1="$(blkid -s UUID -o value /dev/disk/azure/scsi1/lun1)"

# mkdir /data0

# mkdir /data1

# echo "UUID=$UUID0 /data0 ext4 defaults,nofail 0 0" >>/etc/fstab

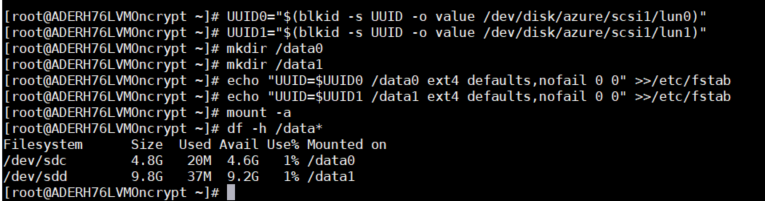
# echo "UUID=$UUID1 /data1 ext4 defaults,nofail 0 0" >>/etc/fstab

**Important:** Replace /data0 and /data1 with your corresponding mount points

* 1. Ensure the LUNs are mounted

# mount -a

# df -h /data\*



**Encrypting the underlying devices**

1. Proceed to encrypt the data disks on this VM executing the following PowerShell script:
   1. Enable disk encryption (In this case we are using Powershell, you can also use CLI)

# Modify all the following parameters accordingly

$rgName = 'VMRGNAME';

$rgKeyName = 'RGKEYNAME';

$vmName = 'VMNAME';

$KeyVaultName = 'KEYVAULTNAME';

$VolumeType = 'Data';

# The following line it's only required if KEK it's used

$ADEKeyName="KEYNAME";

$KeyVault = Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName $rgKeyName;

$diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;

$KeyVaultResourceId = $KeyVault.ResourceId;

# The following 2 lines are only required if KEK it's used

$key = Get-AzureKeyVaultKey -VaultName $KeyVaultName -Name $ADEKeyName

$keyencryptionkeyurl=$key.Id

$sequenceVersion = [Guid]::NewGuid()

# KEK with EncryptFormatAll

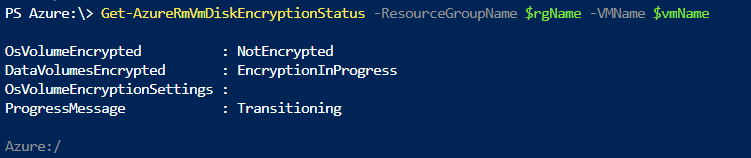
Set-AzVMDiskEncryptionExtension -ResourceGroupName $rgName -VMName $vmName -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -DiskEncryptionKeyVaultId $KeyVaultResourceId -KeyEncryptionKeyUrl $keyencryptionkeyurl -KeyEncryptionKeyVaultId $KeyVaultResourceId -VolumeType $VolumeType -SequenceVersion $sequenceVersion -skipVmBackup -EncryptFormatAll;

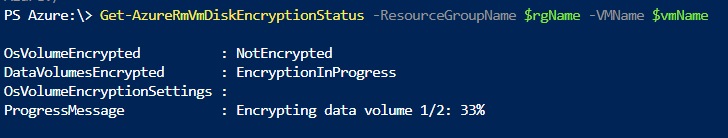
# Without KEK with EncryptFormatAll

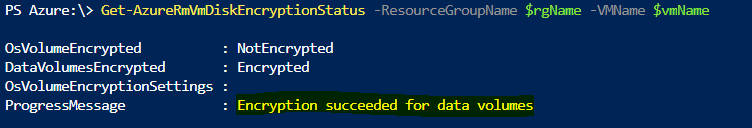
#Set-AzVMDiskEncryptionExtension -ResourceGroupName $rgName -VMName $vmName -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -DiskEncryptionKeyVaultId $KeyVaultResourceId -VolumeType $VolumeType -SequenceVersion $sequenceVersion -skipVmBackup -EncryptFormatAll;

* 1. Check encryption status. You can check status once every 10 minutes, the devices will be encrypted in minutes even if they have a big size since we're using EncryptFormatAll
  2. Wait for the completion status to get into “Encryption succeeded for data volumes” state in the "progressMessage" field.
     1. PowerShell:

Get-AzVmDiskEncryptionStatus -ResourceGroupName $rgName -VMName $vmName ;

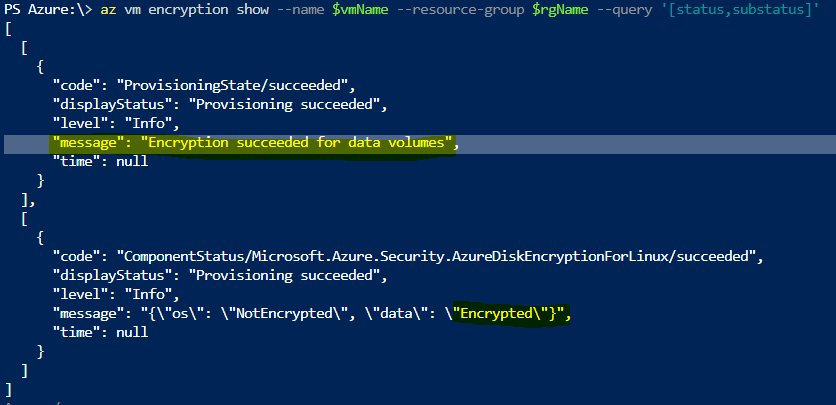






* + 1. AZ CLI:

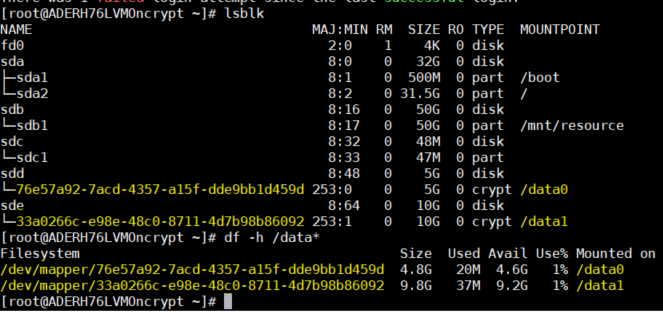
az vm encryption show --name $vmName --resource-group $rgName --query '[status,substatus]'



* 1. You can validate the data disks are mounted (/data1 and /data2) and encrypted with the below commands

# lsblk

# df -h /data\*



* 1. You can notice the file systems were added to */var/lib/azure\_disk\_encryption\_config/azure\_crypt\_mount* (in case of an old encrypion) or added to */etc/crypttab* file in case or a newer encryption.
     1. **Do not** modify any of these files.
     2. This is going to be the file that will be taking care of activating these disks during the boot process so they can be later used by LVM. Do not worry about the /data0 or /data1 mount points, as ADE will lose the ability to get the disks mounted as a normal file system after we do a pvcreate on top of those encrypted devices (which will get rid of the file system format we used during the preparation process).

# cat /var/lib/azure\_disk\_encryption\_config/azure\_crypt\_mount

# cat /etc/crypttab



* 1. Ensure the encrypted LUNs are unmounted so they become available and be used by LVM in the next steps.

# umount /data1

# umount /data2

**Creating LVM structures on top of the encrypted layer(s)**

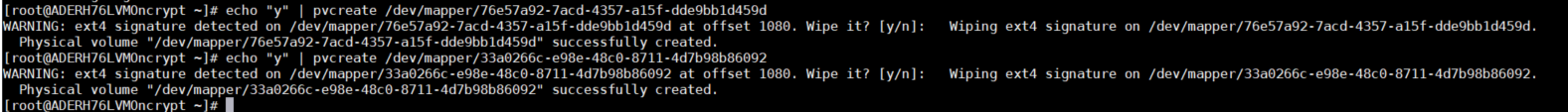
1. Now the underlying disks are encrypted you can proceed to create the LVM structures. Instead of using the device name, use the /dev/mapper paths for each of the disks to perform a pvcreate (on the crypt layer on top of the disk not on the disk itself).
2. Create a Volume group called vgdata(or any other desired name) with 2 volumes lvdata1 and lvdata2 that will be mounted as /data1 and /data2 respectively.
   1. Initialize the PVs, at this moment the encrypted layer will be wiped

# echo "y" | pvcreate /dev/mapper/76e57a92-7acd-4357-a15f-dde9bb1d459d

# echo "y" | pvcreate /dev/mapper/33a0266c-e98e-48c0-8711-4d7b98b86092

**Note:** Replace the dev mappers (/dev/mapper/76e57a92-7acd-4357-a15f-dde9bb1d459d and /dev/mapper/33a0266c-e98e-48c0-8711-4d7b98b86092) accordingly. You can get those from the */var/lib/azure\_disk\_encryption\_config/azure\_crypt\_mount* file, the */etc/crypttab* file or from the *lsblk* command output

You will get a warning asking if it is OK to wipe out the filesystem signature. You may proceed by entering ‘y’ or simply use the echo “y” as shown in the command above.



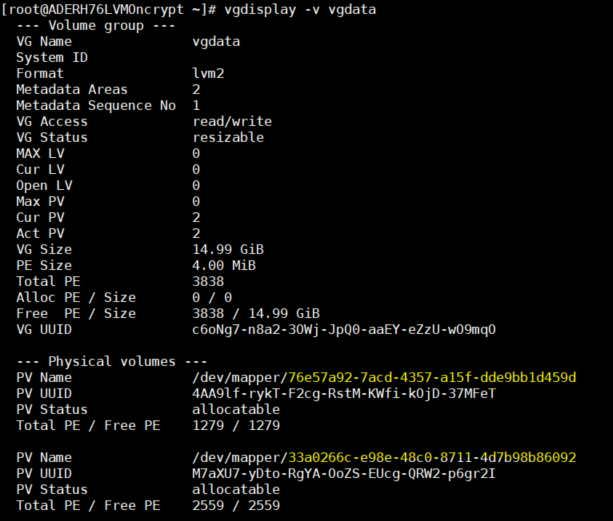
* 1. Create the VG using the same devices already initialized

# vgcreate vgdata /dev/mapper/76e57a92-7acd-4357-a15f-dde9bb1d459d /dev/mapper/33a0266c-e98e-48c0-8711-4d7b98b86092

# vgdisplay -v vgdata

**Note:** Replace the dev mappers (/dev/mapper/76e57a92-7acd-4357-a15f-dde9bb1d459d and /dev/mapper/33a0266c-e98e-48c0-8711-4d7b98b86092) accordingly. You can get those from the */var/lib/azure\_disk\_encryption\_config/azure\_crypt\_mount* file, the */etc/crypttab* file or from the *lsblk* command output

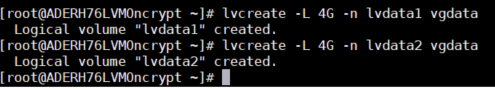




* 1. Create two LVM volumes. In this example we are creating 2 volumes of 4GBs each, they are named lvtest1 and lvtest2

# lvcreate -L 4G -n lvdata1 vgdata

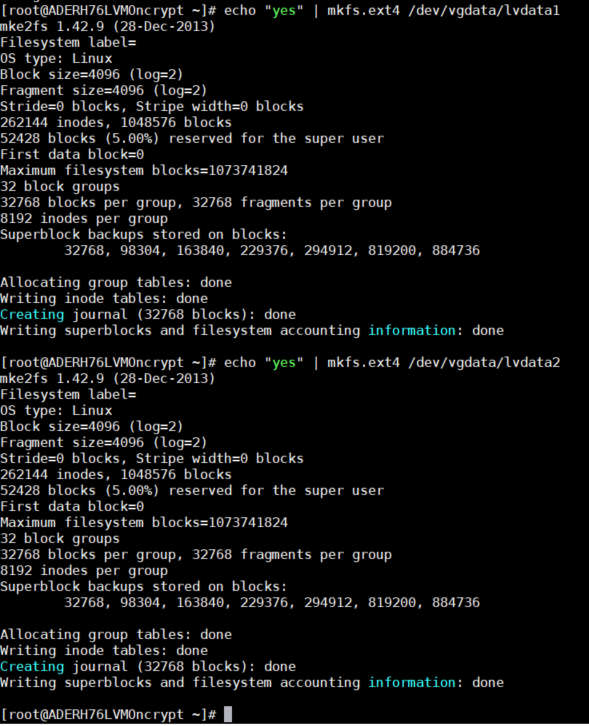
# lvcreate -L 4G -n lvdat



1. Create the file systems over the LVM volumes, in this case ext4 it’s used, you can also use XFS if needed:

# echo "yes" | mkfs.ext4 /dev/vgdata/lvdata1

# echo "yes" | mkfs.ext4 /dev/vgdata/lvdata2



1. Add the new the file systems to /etc/fstab

# echo "/dev/mapper/vgdata-lvdata1 /data0 ext4 defaults,nofail 0 0" >>/etc/fstab

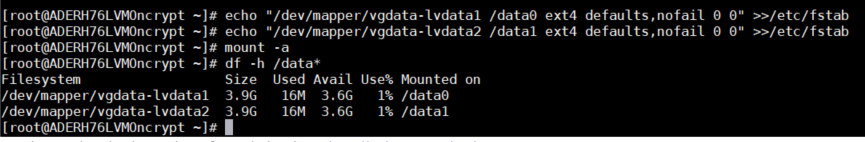
# echo "/dev/mapper/vgdata-lvdata2 /data1 ext4 defaults,nofail 0 0" >>/etc/fstab

# mount -a

**Important:** please make sure the **nofail** option is added to the mount point options of the LVM volumes created on top of an ADE encrypted device. This is very important to avoid the OS from getting stuck during the boot process (or in maintenance mode). The encrypted disk will be unlocked at the end of the boot process and the LVM volumes and file systems will be automatically mounted until they are unlocked by ADE, if the **nofail** option is not used, the OS will never get into the stage where ADE is started and the data disks are unlocked and mounted.

1. Check the file systems are getting mounted

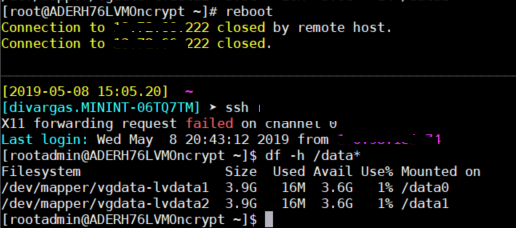
# df -h



1. You can test rebooting the VM and validating the file systems are also automatically getting mounted after boot time. Please take under consideration that this process may take several minutes depending of the amount of file systems and the sizes

# reboot

# df -h /data\*



**Reference**

1. [Use the EncryptFormatAll parameter with Logical Volume Manager (LVM)](https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-linux#--use-the-encryptformatall-parameter-with-logical-volume-manager-lvm)

**ADE Escalation Process**

If the troubleshooting steps found in the wiki don't work please follow the escalation process outlined below:

**ADE Windows Escalation Process:**

1. You can reach out to the Teams Channel [Azure Disk Encryption teams channel](https://teams.microsoft.com/l/channel/19%3ae9617886ec3b4146b6e1ce1f63c4456b%40thread.skype/Ask%2520a%2520SME%2520--%2520Azure%2520Disk%2520Encryption?groupId=90ca5c4d-946f-4250-bb79-6a51561d46e1&tenantId=72f988bf-86f1-41af-91ab-2d7cd011db47) for advise providing the case number, issue description and your question.
2. You can also contact by sending an email to the [Azure Disk Encryption Support DL](mailto:adesup@microsoft.com)
3. For escalation on this feature, please file an [ICM to the Azure Disk Encryption team](http://aka.ms/ADE-ICM-template)
   1. For ***production down*** scenarios, before filing a sev 2 ICM, check this with your TA or ADE SME
   2. Otherwise, file it as sev 3
   3. You can follow up on your ICM sending an email to the [ADE PG](mailto:adeteam@microsoft.com) and [Azure Disk Encryption Support](mailto:adesup@microsoft.com) DLs
   4. In all cases work on getting approval from your TA or ADE SME prior filing an IcM. IcMs should be created to get assistance on product issues rather than normal support issues.

**ADE Linux Escalation Process:**

1. You can reach out to the Teams Channel [Azure Disk Encryption teams channel](https://teams.microsoft.com/l/channel/19%3ae9617886ec3b4146b6e1ce1f63c4456b%40thread.skype/Ask%2520a%2520SME%2520--%2520Azure%2520Disk%2520Encryption?groupId=90ca5c4d-946f-4250-bb79-6a51561d46e1&tenantId=72f988bf-86f1-41af-91ab-2d7cd011db47) for advise providing the case number, issue description and your question.
2. You can also contact by sending an email to the [Azure Disk Encryption Support DL](mailto:adesup@microsoft.com)
3. For escalation on this feature, please [create a **collaboration task** with the Linux Escalation team](https://supportability.visualstudio.com/Azure3rdPartySupport/_wiki/wikis/Azure3rdPartySupport?pageId=189331) using Service Desk
   1. The Linux Escalation Engineers will be taking care of creating any needed ICM with ADE PG: [ICM to the Azure Disk Encryption team](http://aka.ms/ADE-ICM-template)
      1. For ***production down*** scenarios, before filing a sev 2 ICM, check this with your TA or ADE SME
      2. Otherwise, file it as sev 3